IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA,

Plaintiff,

v.

ZACKARY ELLIS SANDERS,

Defendant.

Case No. 1:20-cr-00143
Honorable T.S. Ellis, III
Pretrial conference: Jan. 15, 2021
Filed Under Seal

SUPPLEMENT TO MOTION TO COMPEL

Mr. Sanders, by and through counsel, respectfully submits this supplement in further support of his Motion to Compel the Government to Produce Material, Or, in the Alternative, to Submit Material for *In Camera* Inspection (ECF No. 137).

This supplement and the materials attached hereto further demonstrate that there have always been reasons for the FBI to question the meaning, reliability, and accuracy of the tip it received in this case from the [redacted] ("[redacted]"). Specifically, they further demonstrate that, *inter alia*: (1) the [redacted] never connected Mr. Sanders to the Target Website—but instead the Special Agent merely guessed or assumed there was some connection; and (2) the Special Agent knew when he submitted the Affidavit that there was no evidence of Mr. Sanders's purported activity on any website, despite what Paragraph 23 of the Affidavit clearly suggests.

The defense has uncovered additional documents through its own investigation that demonstrate the Government is continuing to conceal further material discovery. On December 3, 2020, based on that new information, Mr. Sanders sent the Government an additional discovery letter that made three requests. Discovery Letter, attached as Ex. 11. First, Mr. Sanders sought to "clarify whether the [redacted] dated [redacted]—which [Government counsel] informed us the FBI actually received on [redacted]—was redacted by the [redacted], FBI, [Government counsel], or any other government agency." *Id*. at 1. This request was based on the fact that many parts of the [redacted] (attached to ECF No. 51 as Ex. 1) that required a response from the official completing it are blank, including fields related to the reliability of the source and whether the information was suspected to be false. The [redacted] also provided that [redacted] *Id.* Given that the [redacted] was provided to the FBI as a word document, it easily could have been redacted, sanitized, or edited.

Second, Mr. Sanders requested additional information about "accuracy and quality concerns with data produced through [redacted]," the [redacted] operation that the IP address in this case was identified under. *Id.* at 1. Third, because "the documents that purportedly constitute 'the tip' in this case mention both a '[redacted]' and a '[redacted],'" Mr. Sanders requested that the Government clarify its understanding of the differences between the two operations. *Id.* at 2.

On December 4, 2020, Government counsel refused to produce the additional material. Instead of asserting that the requested information did not exist or that the Government did not possess it, the Government claimed that it was not "material or relevant." Email from Government Counsel, attached as Ex. 12. That is incorrect.

Through its own independent investigation, the defense has learned that "[redacted]" included many different websites, not just the Target Website. A [redacted] government report states that "[redacted] is the [redacted]'s project tackling child sexual exploitation offending on the dark web," and that "[a]t any one time there are approximately *70* dark web sites accessible." Inspection Report, attached as Ex. 1, at 11 (emphasis added); *see also* Motion to Compel (ECF No. 137), Ex. 4 (Chief Constable's Update) at 11 ("[redacted] is the [redacted]'s response to *hidden services*, specifically criminally motivated by Child Sexual Abuse and Exploitation *sites and services*") (emphases added). The Government has not produced any discovery explaining what [redacted] is, even though the FBI is clearly part of it, *see infra* at 4-5.

Because [redacted] included numerous websites (at least 70), and because there is no document that connects the IP address associated with Mr. Sanders to any specific website, including one called "[redacted]," there was apparently no basis for concluding that Mr. Sanders ever visited [redacted] or accessed material on it. As Government counsel has admitted, the information from the [redacted] was "limited." Gov't Opp'n (ECF No. 43) at 16. None of that limited information stated that the IP address associated with Mr. Sanders ever even visited any Tor Onion Service website.[1] The most that can be inferred from the tip is that the IP address accessed any one of the other approximately 70 Tor Onion Service websites,[2] a website on the

[1] Even if the Government had evidence that the IP address went to a Tor Onion Service website, the following FBI PowerPoint slide recognizes the many legitimate reasons why someone would do so: for "Secure Communications," "Freedom of Speech," "Political Activism," "Internet Security," and "Internet Privacy." FBI PowerPoint Presentation, attached as Ex. 10.

[2] While there is no evidence of the specific content the Internet user in this case allegedly accessed, the [redacted]'s definition of child sexual abuse and exploitation material, also known as "indecent images of children," can include images where the child is "clothed," and "may" but does not necessarily require that a child be "in a sexual pose" or be "involved in . . . sexual activity." Ex. 8 (Independent Inquiry into Child Sexual Abuse Report) at 10, 13.

open Internet,[3] or some other platform altogether (such as a mobile application, email, or messaging service).[4]

Furthermore, it was known that there were both accuracy and quality concerns with the data produced by the [redacted] generally and through [redacted] specifically. While the "[redacted] must comply with International Standards Organisation (ISO) accreditation, . . . the [redacted] did not meet the ISO standards set by the forensic science regulator in some areas, *including digital forensics*." Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, [redacted] *Inspection: An inspection of the* [redacted] *'s criminal intelligence function* 12 (July 14, 2020), [redacted] (emphasis added).

Issues with the [redacted]'s digital forensics and the accuracy of its data are apparently ingrained. As of August 2019, there were "[c]oncerns in accuracy of data recording" related to child sexual exploitation material, including "identifying the offending" individuals and the incorrect "use of markers." Child Sexual Abuse and Exploitation Assessment, attached as Ex. 2, at 2. That was the same time period when the FBI received the Intel Log (attached to Motion to Compel (ECF No. 37), as Ex. 2), and when the [redacted] was to "review dissemination of packages"

[3] According to a [redacted] statutory inquiry report from March 2020, the [redacted] itself stated in November 2019 "that it was still possible to access known child sexual abuse imagery on '*mainstream* search engines within just '*three clicks*.'" Independent Inquiry into Child Sexual Abuse Report, attached as Ex. 8, at 47 (emphasis in original). That inquiry also found that "[t]he *majority* of websites that host indecent images of children are accessed via the open web." *Id.* at 10 (emphasis added).

[4] *See, e.g.,* Ex. 8 (Independent Inquiry into Child Sexual Abuse Report) at 99 (noting that illegal content can be shared online via WhatsApp, iMessage and FaceTime); *id.* at 46 (explaining that "both app stores and communications services" can be used to access and spread illegal content online).

under [redacted]. *Id.* at 2. In May 2020, it was further confirmed that there were "quality concerns around the products released" under [redacted]. Action Tracker, attached as Ex. 3, at 2. These concerns—which Special Agent Ford knew or should have known—call into question whether the IP address was reliably or accurately identified at all. *See also* Motion to Compel (ECF No. 137) at 19, n.9.

Finally, contrary to what the Government has claimed, it appears that [redacted] was not an "independent" [redacted] investigation. *See* Affidavit ¶ 25; Gov't Opp'n (ECF No. 43) at 1; Gov't Reply (ECF No. 70) at 2, n.1; *see also* Gov't Opp'n (ECF No. 101) at 24 ("The defendant's claim that the United States and the [redacted] were working together to investigate Tor is baseless"). In the U.S. Attorneys' Bulletin, the Government reported that "the global nature of online-facilitated crime . . . means that law enforcement must frequently collaborate with international partners to determine where criminal activity is occurring, as well as how evidence and criminal infrastructure can be seized." U.S. Attorneys' Bulletin, attached as Ex. 4, at 44. Thus, "[i]n recent years, coalitions of United States and foreign law enforcement agencies, frequently led by the Department of Justice, have seized numerous dark markets." *Id.* at 44. For example, in March 2018, U.S. law enforcement and the [redacted] seized a server that was "used to operate a Darknet market [*i.e.* Tor Onion Service website] that exclusively advertised child sexual exploitation videos available for download by members," which "resulted in leads sent to 38 countries and yielded arrests of 337 subjects." Department of Justice Press Release, attached as Ex. 5, at 2. That international investigation was jointly led by U.S. law enforcement "and the [redacted]." *Id.* at 5; *see also* Screenshot of Seized Website, attached as Ex. 6.

At that time, less than a year before the IP address in this case was identified, an indictment from that joint US-[redacted] operation stated that "[t]here was no practical method to

trace a user's actual IP address back through . . . Tor relay computers." Jong Woo Son Indictment, attached as Ex. 7, at 1; *see also* Motion to Suppress No. 4 (ECF Nos. 90-91). The Government's recent acknowledgment of the difficulties that both the US and [redacted] face in de-anonymizing Tor users supports Mr. Sanders's argument that the FBI knew that on May 23, 2019, the [redacted] used [redacted] under the [redacted]—pursuant to [redacted] warrants—to search and seize data from the Internet user's computer, wherever it was located, as well as numerous other computers. *See* Motion to Suppress No. 4 (ECF No. 91); *see also* [redacted] Letter, attached as Ex. 3 to Motion to Compel (ECF No. 37).

Here, [redacted] also involved the [redacted] "[w]orking with partners" to "identif[y] . . . a significant number of unique global [IP] addresses on dark web sites," only "5 percent" of which were "believed to be in the [redacted]." Ex. 1 (Inspection Report) at 11. The FBI was one of those partners. The FBI received an intelligence report as part of [redacted], the [redacted], and another [redacted], this time as part of [redacted] the [redacted] (attached to ECF No. 51 as Ex. 1),[5] which stated it was [redacted] *Id*. Government counsel has also described the [redacted] as "a familiar and reliable foreign counterpart to the FBI." Gov't Opp'n (ECF No. 43) at 16. It appears that here, as in other investigations, the Government has attempted to conceal the international scope of the investigation of Tor Onion Service websites, as its collaboration with the [redacted] would, *inter alia*, present a Fourth Amendment issue due to the warrantless intrusion upon Mr. Sanders's computer via a Network Investigative Technique. *See, e.g.,* Internal FBI Email, attached as Ex. 9

[5] The Government informed defense counsel that October 25, 2019, was the date that the FBI received the [redacted], as the [redacted] itself does not indicate that this was the date that the [redacted] was generated or sent. However, a newly discovered document by the defense, Ex. 3 (Action Tracker) states it was only on March 5, 2020, that the [redacted] confirmed that there would be a second version of [redacted]. Ex. 2 at 2.

(discussing information that the FBI "want[ed] to continue to protect," that had "not been disclosed in any filings" or to the defense, including the "scope of the international aspect of the [Playpen] investigation").

Under *Brady*, Rule 16, and prosecutors' ethical obligations, the Government should have produced the substance of the requested information long ago. The documents the defense has uncovered show that the Government is continuing to conceal yet other *Brady* material helpful to Mr. Sanders. The Government should produce all related material either to Mr. Sanders or, in the alternative, to this Court for *in camera* inspection.

Respectfully submitted,

/s/ Jonathan Jeffress

Jonathan Jeffress (#42884)
Emily Voshell (#92997)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: evoshell@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

Counsel for Defendant Zackary Ellis Sanders

CERTIFICATE OF SERVICE

I hereby certify that on this 5th day of December 2020, the foregoing was served electronically on the counsel of record through the U.S. District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

/s/ Jonathan Jeffress
Jonathan Jeffress